附件 9

信息系统突发事件应急预案

一、总则

1、为进一步做好学校信息系统网络与信息安全事件的应急工作，根据国家关于计算机信息系统安全有关规定，特制定本规定。

2、信息系统网络与信息安全事件指危害信息系统系统安全、影响系统正常使用、或系统发生信息泄露的事件。

二、事件内容与等级划分

1、网络与信息安全事件具体内容包括：

（1）系统的文档数据遭到破坏、篡改或窃取。

（2）系统硬件受到破坏性攻击不能正常发挥其部分功能或全部功能。

（3）系统软件受到破坏性攻击不能正常发挥其部分功能或全部功能。

（4）系统软件受到计算机病毒的侵害，局部或全部数据和功能受到损坏，使系统不能工作或工作效率急剧下降。

（5）系统的物理设备被人为毁坏，无法正常工作。

（6）系统受到自然灾害的破坏，如：地震、水灾、火灾、雷电、台风。

（7）其他信息安全事件。

2、网络与信息安全事件的等级划分

根据网络与信息安全突发公共事件的可控性、严重程度和影响范围，可分为以下四级：

级别	条件	影响范围	控制事态的能力
I级（特别重大）	发生严重有害程序事件、网络攻击事件、设备设施故障、灾害性事件造成全校大面积网络与信息系统瘫痪； 发生严重信息内容安全事件和信息破坏事件；	对学校正常工作造成特别严重损害	事态发展超出学校控制能力的安全事件
II级（重大）	发生有害程序事件、网络攻击事件、设备设施故障、灾害性事件造成全校性网络与信息系统瘫痪； 发生信息内容安全事件和信息破坏事	对学校正常工作造成严重损害	事态发展超出技术部门控制能力，需要学校各部门协同处置的安全事件

	件；		
III级（较大）	发生有害程序事件、网络攻击事件、设备设施故障、灾害性事件造成学校某一区域网络与信息系统瘫痪；	对学校正常工作造成一定损害	信息化办公室可处理的安全事件
IV级（一般）	发生有害程序事件、网络攻击事件、设备设施故障、灾害性事件造成学校某一局部网络与信息系统故障	对学校某些工作造成影响，但不危及学校整体工作	信息化办公室可处理的安全事件

3、应急处置、事件调查与评估

（1）网络与信息安全事件的处置原则

网络与信息安全事件应急处置，依照“统一领导，快速反应，密切配合，科学处置”的组织原则和“谁主管谁负责、谁运行谁负责、谁使用谁负责”的协调原则，充分发挥各方面力量，共同做好网络与信息安全事件的应急处置工作。

（2）组织机构及职责

网络安全与信息化事故处置工作小组：

组　长：分管信息化工作的副校长

副组长：信息化办公室主任

组　员：相关部门主管组成。

全校网络与信息安全事件应急处置工作由学校网络安全与信息化领导小组统一指导、指挥、协调。各相关单位须坚决执行领导小组的决定，密切配合，履行职责。

（3）相关职责

组织机构	职责
网络安全与信息化领导小组	1. 决定Ⅰ级和Ⅱ级网络与信息安全事件应急预案的启动。 2. 督促检查安全事件处置情况及各有关单位在安全事件处置工作中履行职责情况。 3. 对全校各单位贯彻执行应急处置预案、应急处置准备情况进行督促检查。
党委校长办公室	1. 组织协调有关部门查处利用计算机网络泄密的违法行为。 2. 牵头组织重大敏感时期、重要活动、重要会议期间发生的信息安全事件的协调处置。

信息化办公室 网络、软件中心	1. 负责校园基础网络系统安全。 2. 负责计算机病毒疫情和大规模网络攻击事件的处置。 3. 负责校级网络与信息系统安全事件处置的技术支持。
党委宣传部 团委 学生工作部 研究生工作部	1. 负责学校舆情监测，对于涉及师生政治思想方面的倾向性、苗头性问题加强分析研判。 2. 负责舆情突发事件的处置。 3. 负责应急处置过程中的舆论处置。
保卫处	1. 密切配合公安部门，做好网络与信息安全事件的处置工作。
其他部门	1. 负责本单位内部的网络与信息安全管理和突发事件应急处置，对照本预案建立单位内部应急处置机制。 2. 配合各单位落实相关应急处置措施。

4、网络与信息安全事件的处理

（1）信息泄露事件的处理

发现或接到报告后，应在第一时间内组织力量切断信息

泄露源头、重新对系统进行风险评估，并及时修补系统安全漏洞，防止重复出现此类事件。

信息泄露事件处置后，安全管理员应做好事件处置相关记录。

（2）安全事件的处理

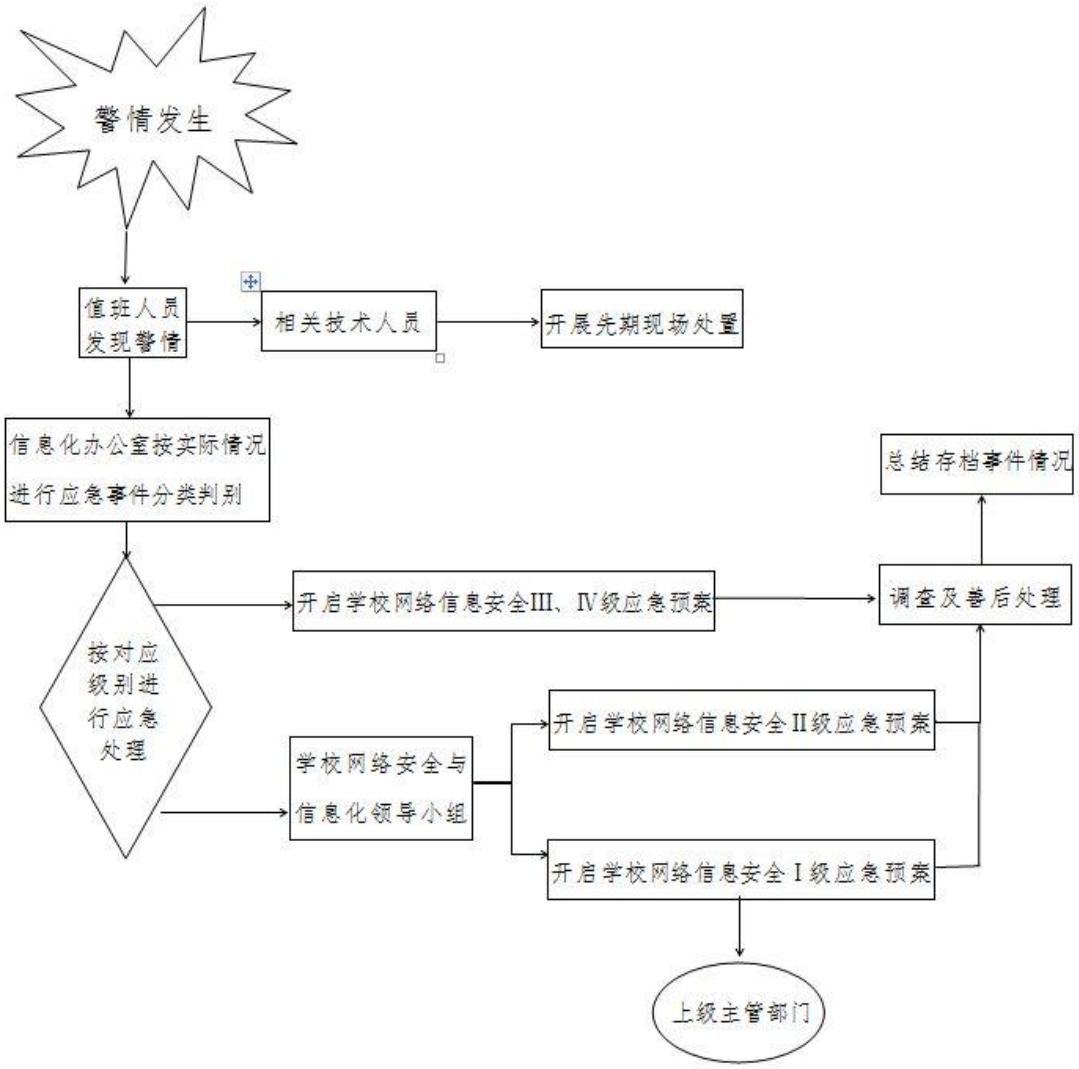
当发现网络型病毒，造成网络阻塞及网络风暴，影响整个信息系统的正常工作时，要及时升级杀毒软件的病毒库，并针对操作系统、软件漏洞升级安全补丁，进行系统全面的查杀病毒。必要时，切断网络联接，对网络局部进行杀毒，确保局部无病毒后再联通全部网络。当发现网络攻击或其它异常行为时，及时采取封堵可疑 IP、关闭相关端口、保护涉密信息等措施。

当发生网络硬件设备、安全设备及服务器故障或损坏情况时，应及时通知设备供应商，在 8 小时内解决相关问题。

当出现信息系统故障或崩溃情况时，应及时利用备份数据进行恢复，保障网络正常运转。

对于能力范围内不能解决的，应立即邀请具备条件的单位进行技术协助。

对于上述处理过程，应急处置人员要进行详细记录。



（3）处理流程

5、网络与信息安全事件的评估改进

对于产生严重后果的突发事件，应急处置工作结束后，学校应组织有关人员和技术专家组成事件调查组，对事件发生原因、性质、影响、后果、责任及应急处置能力、恢复重建等问题进行全面调查评估，形成网络与信息安全事件处理报告。报告内容包括：

（1）问题或故障；

（2）原因分析；

（3）采取的应急措施或应急方案；

（4）结果评价；

（5）建议应采取的后续措施或需进一步考虑的解决方案；

（6）总结经验教训。

事件的调查处理和总结评估工作原则上在应急响应结束后30天内完成。

三、应急计划

1、学校各学院（部门）应针对各类网络与信息安全事件制定行之有效的应急计划。

（1）应急计划应条理清楚、语言简洁、步骤分明、具有强可操作性。

（2）应急计划应有多种备用方案，每种方案均可独立实施，应有各种方案的优先排序。

（3）应急计划应有明确的负责人与各级责任人的职责。

（4）应急计划应便于培训和实施演习。

（5）应急计划简单流程图应公布在显著和方便的位置，以便发生事故时，能迅速、方便地执行。

2、应急计划应包括紧急措施、资源备用、恢复过程、演习和应急计划关键信息。具体如下：

（1）紧急措施

制定对各种网络与信息安全事件的响应规程、抢救计划、救护计划和撤离计划，以保护人员生命，降低财产损失。

（2）资源备用

软件资源备用：对每一信息系统需要有足够备份，并将备份存放于免受攻击或受灾害影响的地方。

电源备用：应配置不间断电源，一般不间断电源应可在断电后维持工作二小时以上。应配置备用交流稳压电源。重要系统和大型系统应配备多种供电来源。

经费保障：信息化办公室应根据校园网络与信息系统安全预防和应急处置工作的实际需要，申报网络与信息系统关键设备及软件的运维专项资金，提出本年度应急处置工作相关设备和工具所需经费，上报至财务处纳入年度预算，由学校给予资金保障。

重要或大型系统中的关键设备和信息安全产品应采用双机热备份。

对特别重要信息应尽可能采取安全保密的异地备份措施。

（3）恢复过程

首先恢复重要的安全产品，保证系统安全情况下，其次恢复应用系统。

（4）培训和演习

应每年进行应急计划的培训和演习，使每个工作人员熟

悉应急知识和在应急计划中应采取的措施和应负的责任，以利于紧急事故出现时能迅速执行应急计划。

（5）应急计划关键信息

应急计划关键信息应张贴在显著和方便的位置，应急计划关键信息包括：火警电话、报警电话、应急负责人电话等。

四、应急宣传、演练、培训

1、充分利用学校各种传播媒介及有效形式，加强突发网络安全事件预防和处置的有关法律、法规和政策的宣传，开展网络安全基本知识和技能的宣传活动。

2、各学院（部门）应当在信息化办公室指导下每年至少组织一次对系统用户进行安全应急培训和应急演练，并根据演练结果对应急预案进行评审和修订。

3、发生应急事件并处理完成后，各学院（部门）应当对事件进行分析总结，进行风险评估，改进不足，弥补漏洞。

4、各学院（部门）应加强对网络与信息安全等方面专业技能的培训，指定专人负责安全技术工作。